



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,159	10/30/2000	Anup K. Ghosh	CIG-103	7526
7590	04/10/2006		EXAMINER	
Brett C. Martin 1650 Tyson Blvd. McLean, VA 22102			TRAN, ELLEN C	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/698,159	GHOSH ET AL.	
Examiner Ellen C. Tran	Art Unit 2134		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 22 December 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 23-30,33-44 and 47-50 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 23-30,33-44 and 47-50 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____

5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

DETAILED ACTION

1. This action is responsive to communication: 22 December 2005, the original application was filed on 30 October 2000 with a continuing application priority date of 28 October 1999.
2. Claim 23-30, 33-44, and 47-50 are currently pending in this application. Claims 23 and 37 are independent claims. Claims 37 has been amended. Claims 1-22, 31, 32, 45, and 46 have been cancelled.

Response to Arguments

3. Applicant's arguments with respect to claims 23-30, 33-44, and 47-50 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 23-30, 33-44, and 47-50**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Munson et al. U.S. Patent No. 6,681,331 (hereinafter '331) in view of Botros et al. US Patent No. 6,769,066 (hereinafter '066).

As to independent claim 37, "A method for detecting intrusive behavior" is taught in '331 col. 2, lines 10-11;

"in a session on a computer during an application monitoring phase, said session comprising a plurality of applications invoked on said computer, and said computer having

a computer operating system, said method comprising the steps of: (a) training a plurality of neural networks during a training phase, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications” is shown in ‘331 col. 4, lines 33-40 (the “training phase” is interpreted as the “calibration process” / the “neural network(s)” are interpreted to be the same as “profile(s)” / the “application profile(s)” are interpreted as “software module(s)”);

“(b) creating a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session” is taught in ‘331 col. 7, lines 17-34 and col. 9, lines 49-55;

“(c) performing a temporal locality identifying algorithm, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of neural networks the neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive” is taught in ‘331 col. 4, lines 26-65 (the “performing a temporal locality identifying algorithm” is interpreted as “the operation of an execution profile comparator” / “pre-determined criteria” is interpreted as “boundary condition” and “predetermined threshold” / “labeled intrusive” interpreted as “then a level 2 alarm 503 is raised, indicating a certainty of an intrusive attack”)

the following is not taught in '331: "**(b) selecting for use one or more trained neural networks based upon performance during a testing phase**" however '066 teaches "In one embodiment, the model is trained using a neural network algorithm. In another embodiment, a probability factor for use in determining the ratio of anomalous feature values and normal feature values is derived. In another embodiment, an anomalous feature data list from numerous anomalous feature values is randomly selected. Similarly, a normal feature data list from numerous normal feature values is randomly selected. In yet another embodiment, a desired score is assigned for the selected feature data list used as input to the model" in col. 3, line 63 through col. 4, line 34.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '119 a neural network that detects intrusive behaviors to include a means to select the trained neural model based on selection during the training phase. One of ordinary skill in the art would have been motivated to perform such a modification because prior security system have many drawbacks such as cumbersome and overly complex set of rules need to be entered as indicated by '660 (see col. 2, line 30 through col. 3, line 19). "As stated above, these thresholds can be outdated or moot if circumstances change in the system. For example, circumstances can change and the restricted file mentioned above can be made accessible to a larger group of users. In this case an expert would have to modify the rules in expert system 14. As mentioned above, the feature and expert system components as shown in FIG. 1 and conventional models used in conjunction with these components have significant drawbacks ... Therefore, it would be desirable to utilize a features list generator in place of a traditional expert system that can automatically update itself to reflect changes in user and user group current behavior. It would also be desirable to derive a training process for a model used in conjunction

with a features generator to generate a score reflective of changing user behavior. It would also be desirable to have the training process or algorithm accurately read anomalous user behavior. Furthermore, it would be desirable to have such a features generator be self-sufficient and flexible in that it is not dependent on changes entered by an expert and is not a rigid rule-based system”.

As to dependent claim 38, “wherein the second session comprises non-intrusive behavior” is shown in ‘331 col. 4, lines 30-33.

As to dependent claim 39, “wherein the application data comprises a distance between a sequential mapping of system calls made by a corresponding one of the plurality of applications and a pre-defined string of system calls” is disclosed in ‘331 col. 4, lines 26-40.

As to dependent claim 40, “wherein the application data comprises a distance between a sequential mapping of object request made by a corresponding one of the plurality of applications and a pre-defined string of object requests” is shown in ‘331 col. 7, line 62 through col. 8, line 48.

As to dependent claim 41, “wherein the plurality of application profiles is created by a data pre-processor application” is disclosed in ‘331 col. 4, lines 33-40.

As to dependent claim 43, “wherein the data pre-processor creates the second plurality of application profiles in real-time” is taught in ‘331 col. 6, lines 11-12.

As to dependent claim 44, “wherein the plurality of trained neural networks receive input from the plurality of application profiles in a real-time” is taught in ‘331 col. 6, lines 11-12.

As to dependent claim 47, “wherein the plurality of trained neural networks comprises a plurality of backpropogation neural networks” is taught in ‘331 col. 10, lines 8-63 (“trained neural networks” interpreted as “nominal profiles” / “backpropogation neural networks” interpreted as “module profile(s)”).

As to dependent claim 48, “wherein each backpropogation neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer” is taught in ‘331 col. 14, lines 47-67 (“input layer” interpreted as “user operations”, “hidden layer” interpreted as “computer analysis/calculations performed by comparator” / “output layer” interpreted as “indication of an alarm condition or normal”).

As to dependent claim 49, “wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each neural network in the plurality of backpropogation neural networks and selecting the case wherein the corresponding neural network has a highest accuracy rate” is taught in ‘331 col. 6, lines 26-56 (“number of nodes in the hidden layer” interpreted to be the “sampling rate”).

As to dependent claim 50, “wherein the plurality of neural networks comprises a plurality of recurrent neural networks” is taught in ‘331 col. 9, lines 55-67.

As to independent claim 23, this claim is directed to the detection system of the method of claim 37 and is similarly rejected along the same rationale.

As to dependent claims 24-29 and 32-36 these claims incorporate substantially similar subject matter as in cited in claims 38-44 and 47-50 above and are rejected along the same rationale.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT
Ellen. Tran
Patent Examiner
Technology Center 2134
1 April 2006

Jacques H. Louis-Jacques
Jacques H. Louis-Jacques
Patent Examiner
Technology Center 2134